



Intelligence Analysis for Strategic Risk Assessments

May 14, 2008

Terrorism and Threat Analysis

Operation Crevice

- Plot in the UK
- Tip from an employee at a rental storage business
- UK authorities have an idea of the attack method, the time frame, and potential targets
 - Pubs, night clubs
 - Trains
 - Shopping centers

Tactical Threat Analysis

If authorities can identify the terrorist operation before the attack, there are multiple courses of action

- Eliminate immediate threat
- Allow to continue to identify support and planning network
- Decrease vulnerabilities
- Issue warnings

Limitations of Tactical Analysis

Tactical analysis may not indicate

- What other cells may target
- The maturity or timeframe of other plots
- The other capabilities that the larger group may possess
- The strategic goals of the larger organization
- The tactical goals of other cells

Difficulty of Strategic Threat Assessment

- Strategic threat supports longer-term planning than tactical analysis
- Cannot simply extrapolate from one plot
- Cannot create simplified rules
- To plan, organizations must know what type of attack to plan for, and whether they may be targeted

Key to the warning challenge is that the substantive uncertainty surrounding threats to US interests requires analysts, and policymakers, to make judgments that are inherently vulnerable to error.

Analysts must issue a strategic warning far enough in advance of the feared event for US officials to have an opportunity to take protective action, yet with the credibility to motivate them to do so. No mean feat.

Waiting for evidence the enemy is at the gate usually fails the timeliness test; prediction of potential crises without hard evidence can fail the credibility test. When analysts are too cautious in estimative judgments on threats, they brook blame for failure to warn. When too aggressive in issuing warnings, they brook criticism for “crying wolf.”

- Jack Davis, “Improving CIA Analytic Performance: Strategic Warning”
2002

Supporting Strategic Risk Assessments

To form a strategy to reduce the risk from terrorist attacks, decision-makers need a threat assessment based on intelligence and supporting evidence so that they can

- compare the severity of several threats,
- understand the degree of certainty in the assessment, and
- determine the potential for change.

Yet, in the political arena, invulnerability *is* the standard by which homeland security policies are judged. Washington think tanks, federal agencies, and government commissions have produced a steady stream of reports since 9/11 detailing the myriad vulnerabilities of the homeland and the insufficiency of the government response before and after 9/11. The attack scenarios they present demonstrate a degree of imaginative thinking that even the innovative strategists of Al Qa'eda could never match. Moreover, the scenarios are often connected only to vulnerabilities, not to threats. Each type of attack is said to be plausible, regardless of whether any particular actor in the world has both the desire and the capacity to carry it out. A vaguely defined enemy, usually labeled 'Al Qa'eda,' is assumed to be willing and capable of doing essentially anything.

- Jeremy Shapiro, “Managing Homeland Security: Develop a Threat-Based Strategy,” 2008.

The Problem with Experts

According to experts, the U.S. should be concerned about nuclear attack by sea. More than 85 non-proliferation and national-security experts polled for a congressional study estimate that the risk of a WMD attack in the next decade using some sort of nuclear device is as high as 70 percent.

- Veronique de Rugy, “Is Port Security Spending Making Us Safer?” 2005

Initial Attempts at Quantification

<p>Weighting of DHS - FY2006 Risk Formula</p>	<p>Risk is calculated for both geographic areas and assets. While both calculations include T, V, and C factors, they have distinct subcategories.</p> <p><u>Geographic</u> <i>Threat (T)</i> - (IC reports, FBI investigations, ICE investigations, suspicious incidents, I-94 visitors from countries of interest, total # of visitors from such countries with state as destination) <i>Vulnerability (V)</i> - (total # international visitors, miles of international border, miles of designated WIPP route) <i>Consequence (C)</i> - (human health, economic, strategic mission, and psychological - as well as numerous subsets of each)</p> <p><u>Asset</u> <i>Threat (T)</i> (strategic intent, 'chatter,' attractiveness of target, capabilities) <i>Vulnerability (V)</i> (value assigned by DHS) <i>Consequence (C)</i> (human health, economic, strategic mission, and psychological)</p> <p>It is not clear how each factor and sub-factor were weighted.^d</p>
--	--

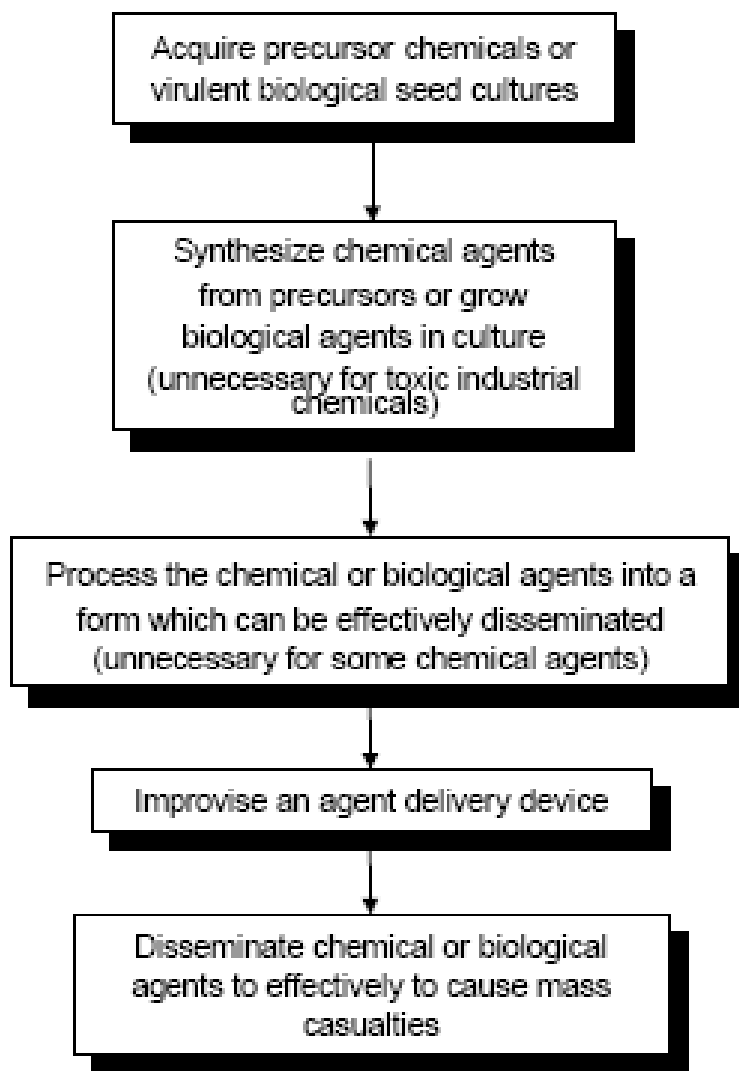
- Congressional Research Service, "The Department of Homeland Security's Risk Assessment Methodology: Evolution, Issues, and Options for Congress," 2006.

Table 1-3: Criteria to Select Primary Threats

Criteria							
Scenario	Access to Agent	Knowledge/Expertise	History of Threats (Building Functions/Tenants)	Asset Visibility/Symbolic	Asset Accessibility	Site Population/Capacity	Collateral Damage/Distance to Building
9-10	Readily available	Basic knowledge/open source	Local incident, occurred recently, caused great damage; building functions and tenants were primary targets	Existence widely known/iconic	Open access, unrestricted parking	> 5,000	Within 1,000-foot radius
6-8	Easy to produce	Bachelor's degree or technical school/open scientific or technical literature	Regional/State incident, occurred a few years ago, caused substantial damage; building functions and tenants were one of the primary targets	Existence locally known/landmark	Open access, restricted parking	1,001-5,000	Within 1-mile radius
3-5	Difficult to produce or acquire	Advanced training/rare scientific or declassified literature	National incident, occurred some time in the past, caused important damage; building functions and tenants were one of the primary targets	Existence publish/well-known	Controlled access, protected entry	251-1,000	Within 2-mile radius
1-2	Very difficult to produce or acquire	Advanced degree or training/classified information	International incident, occurred many years ago, caused localized damage; building functions and tenants were not the primary targets	Existence not well-known/no symbolic importance	Remote location, secure perimeter, armed guards, tightly controlled access	1-250	Within 10-mile radius



Figure 1: Stages for Terrorists Working Outside a State-run Laboratory to Conduct Chemical and Biological Terrorism



Source: GAO, on the basis of analysis and discussion with chemical and biological warfare experts.

Bayesian Probability

	Hypothesis A	Hypothesis B	Hypothesis C
Period 1	0.07	0.42	0.51
Period 2	0.08	0.78	0.15
Period 3	0.0	0.37	0.63

- Jessica McLaughlin and M. Elisabeth Paté-Cornell, "A Bayesian Approach to Iraq's Nuclear Program Intelligence Analysis: A Hypothetical Illustration," 2005.

Level of Severity

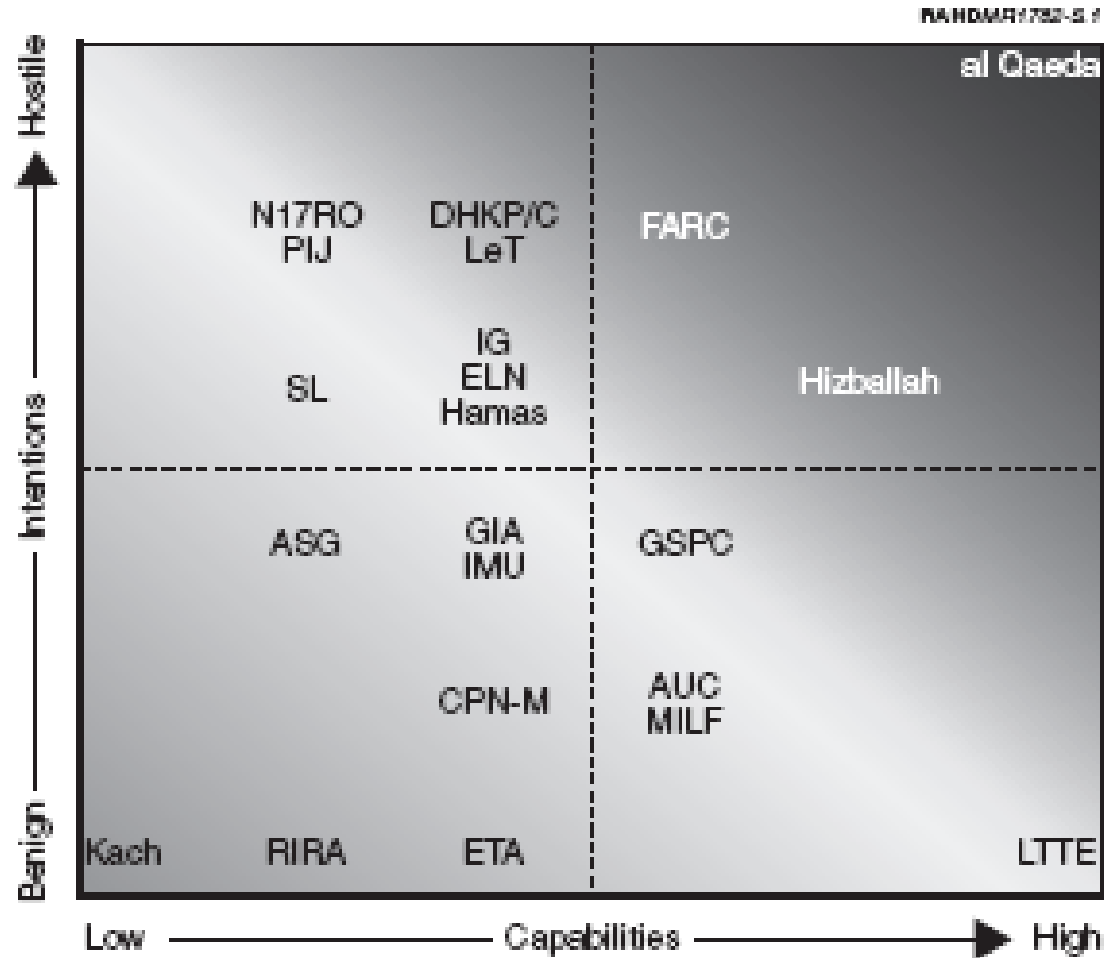


Figure S.1—Understanding the Relative Threats Posed by Terrorist Groups

Evidence-Based Threat Analysis

- Evidence-based threat analysis should be the first tool that decisionmakers use to assess threat for comparative risk
- A system should be able to discriminate the severity of threat
 - from multiple groups,
 - from multiple attack methods,
 - to multiple facilities

Complementing Evidence-Based Analysis

- Red cell analysis
 - pursue alternative hypotheses
 - greater degree of flexibility
- Red team exercises
 - investigate assumptions
 - useful for analyzing a persistent threat
- Game theory
 - useful for analyzing an adversary pursuing a type of effect

Threat Analysis Tool Kit

- Evidence-based analysis
 - Reveals what we know
 - Relies on justifying conclusions
 - Sets the baseline for prioritizing scenarios
- Imagination-based analysis
 - Explores possibilities
 - Allows decisionmakers to see areas of uncertainty and how things may change
 - Allows the hedging of bets

GMU: Elements of Risk

- This topic was written in support of the George Mason University Critical Infrastructure Protection program
- The monograph *Elements of Risk* is available on the CIP Program website at http://cipp.gmu.edu/research/CIP_Risk_Monograph.php.